FORM PTO-1390 U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE

TRANSMITTAL LETTER TO THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US) CONCERNING A FILING UNDER 35 U.S.C. 371

ATTORNEY'S DOCKET NUMBER
1454.1053/MJH

09/806435

INTERNATIONAL APPLICATION NO.	INTERNATIONAL FILING DATE	PRIORITY DATE CLAIMED
PCT/DE99/02844	September 8, 1999	September 30, 1998

TITLE OF INVENTION
METHOD AND SYSTEM FOR UPDATING A PASSWORD

APPLICANT(S) FOR DO/EO/US
Steffen FRIES et al.

Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information:

1. [X] This is a **FIRST** submission of items concerning a filing under 35 U.S.C. 371.
2. [X] This is an express request to immediately begin national examination procedures (35 U.S.C. 371(f)).
3. [ ] The US has been elected by the expiration of 19 months from the priority date (PCT Article 31).
4. [X] A copy of the International Application as filed (35 U.S.C. 371(c)(2))
   a. [X] is transmitted herewith (required only if not transmitted by the International Bureau).
   b. [ ] has been transmitted by the International Bureau.
   c. [ ] is not required, as the application was filed in the United States Receiving Office (RO/US).
5. [X] A translation of the International Application into English (35 U.S.C. 371(c)(2)).
6. [ ] Amendments to the claims of the International Application under PCT Article 19 (35 U.S.C. 371(c)(3))
   a. [ ] are transmitted herewith (required only if not transmitted by the International Bureau).
   b. [ ] have been transmitted by the International Bureau.
   c. [ ] is not required, as the application was filed in the United States Receiving Office (RO/US)
7. [ ] A translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371(c)(3)).
8. [X] An oath or declaration of the inventor (35 U.S.C. 371(c)(4)).
9. [X] A translation of the Annexes to the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 371(c)(5)).

Items 10-15 below concern document(s) or information included:

10. [ ] An Information Disclosure Statement Under 37 CFR 1.97 and 1.98.
11. [X] An assignment document for recording.
    Please mail the recorded assignment document to:
    a. [X] the person whose signature, name & address appears at the bottom of this document.
    b. [ ] the following:
12. [X] A preliminary amendment.
13. [X] A substitute specification
14. [ ] A change of power of attorney and/or address letter.
15. [X] Other items or information:

2. [X] The U.S. National Fee (35 U.S.C. 371(c)(1)) and other fees as follows:

CLAIMS	(1) FOR	(2) NUMBER FILED	(3) NUMBER EXTRA	(4) RATE	(5) CALCULATIONS
	TOTAL CLAIMS	23 -20=	3	x $ 18.00	60.00
	INDEPENDENT CLAIMS	3 -3=	0	x $ 80.00	0.00
	MULTIPLE DEPENDENT CLAIM(S) (if applicable)			+ $270.00	0.00
	BASIC NATIONAL FEE (37 CFR 1.492(a)(1)-(4): [ ] Neither international preliminary examination fee (37 CFR 1.482) nor international search fee (37 CFR 1.445(a)(2)) paid to USPTO..............$1,000 [X] International preliminary examination fee (37 C.F.R. 1.482) not paid to USPTO but International Search Report prepared by the EPO or JPO.. . ...$ 860 [ ] International preliminary examination fee (37 C.F.R. 1.482) not paid to USPTO but international search fee (37 C.F.R. 1.445(a)(2) paid to USPTO..................$ 710 [ ] International preliminary examination fee paid to USPTO (37 CFR 1.482) but all claims did not satisfy provision of PCT Article 33(1)-(4).............$ 690 [ ] International preliminary examination fee paid to USPTO (37 CFR 1.482) and all claims satisfied provisions of PCT Article 33(2) to (4)................$ 100				860.00
	Surcharge of $130 for furnishing the National fee or oath or declaration later than [ ] 20 [X] 30 mos. from the earliest claimed priority date (37 CFR 1.482(e)).				
			TOTAL OF ABOVE CALCULATIONS		920.00
	Reduction by 1/2 for filing by small entity, if applicable. Affidavit must be filed also. (Note 37 CFR 1.9, 1.27, 1.28.)				
			SUBTOTAL		920.00
	Processing fee of $130 for furnishing the English Translation later than [ ] 20 [ ] 30 mos. from the earliest claimed priority date (37 CFR 1.482(f)).				
			TOTAL NATIONAL FEE		920.00
	Fee for recording the enclosed assignment (37 CFR 1.21(h)).				40.00
			TOTAL FEES ENCLOSED		960.00

a. [X] A check in the amount of $960.00 to cover the above fees is enclosed.

b. [ ] Please charge my Deposit Account No. 19-3935 in the Amount of $ to cover the above fees. A duplicate copy of this sheet is enclosed.

c. [X] The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to Deposit Account No. 19-3935. A duplicate copy of this sheet is enclosed.

21171
PATENT TRADEMARK OFFICE

March 30, 2001
DATE

NAME: Mark J. Henry
REGISTRATION NO.: 36,162

Docket No. 1454.1053/MJH

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:

Steffen FRIES et al.

Serial No.: NEW　　Group Art Unit: To be assigned

Filed: March 30, 2001　　Examiner: To be assigned

For: METHOD AND SYSTEM FOR UPDATING A PASSWORD

PRELIMINARY AMENDMENT

Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

Before examination of the above-identified application, please amend the application as follows:

IN THE SPECIFICATION

Please REPLACE the pending specification with the SUBSTITUTE SPECIFICATION attached hereto.

IN THE ABSTRACT

Please REPLACE the originally filed Abstract with the enclosed Substitute Abstract.

IN THE CLAIMS

Please **CANCEL** claims 1-12 without prejudice or disclaimer of any of the subject matter claimed therein.

Please **ADD** new claims in accordance with the following:

13. (NEW) A method for updating a password between a first computer and a second computer, comprising:

receiving at the second computer a service request message transmitted by the first computer over a communication link existing between the first computer and the second computer, the service request message containing the password, and being used to request provision of a service;

checking, at the second computer, whether the password contained in the service request message is valid for the first computer;

if the password is valid, providing the service;

if the password is invalid, transmitting from the second computer to the first computer an update message to request that the password be updated; and

forming an updated password.

14 (NEW) The method as claimed in claim 13, wherein after the updated password is formed, the service request message transmitted by the first computer to the second computer contains the updated password and the second computer checks whether the updated password is valid.

15. (NEW) The method as claimed in claim 13, wherein the updated password is formed in the following manner:

the first computer transmits to the second computer a password message containing the updated password, such that the updated password can be ascertained only by using the password,

the second computer uses the password to ascertain the updated password from the password message, and

the second computer stores the updated password.

16. (NEW) The method as claimed in claim 15, wherein the password message contains the updated password in an encrypted form, the key for encrypting the updated password being formed on the basis of the password.

17. (NEW) The method as claimed in claim 16, wherein the key is formed by stringing together the password a number of times.

18. (NEW) The method as claimed in claim 15, wherein the second computer transmits an acknowledgment message to acknowledge the use of the updated password within the context of the communication link.

19. (NEW) The method as claimed in claim 13, wherein before the second computer checks whether the password is valid, the second computer authenticates the first computer using an authentication token for the first computer, which is contained in the service request message.

20. (NEW) The method as claimed in claim 13, wherein the check to determine whether the password contained in the service request message is valid is performed using a monitor database indicating whether the second computer has previously transmitted an update message to the first computer.

21. (NEW) The method as claimed in claim 13, wherein

the service request message contains a statement relating to integrity protection,

the second computer checks the received service request message for its integrity,

the password is checked only if the integrity of the service request message is ensured, and

if the integrity of the service request message is not ensured the requested service is refused.

22. (NEW) A system for updating a password between first and second computers, comprising:

a receiving unit to receive at a second computer a service request message transmitted by the first computer over a communication link existing between the first computer and the second computer, the service request message containing the password, and being used to request provision of a service;

a checking unit to check at the second computer, whether the password contained in the service request message is valid for the first computer;

a providing unit to provide the service requested if the password is valid;

a transmission unit to transmit, if the password is invalid, an update message from the second computer to the first computer, the update message being used to request that the password be updated; and

a forming unit to form an updated password.

23. (NEW) The system as claimed in claim 22, wherein after the updated password is formed, the service request message transmitted by the first computer to the second computer contains the updated password and the second computer checks whether the updated password is valid.

24. (NEW) The system as claimed in claim 22, wherein the forming unit comprises:

a transmit unit at the first computer to transmit to the second computer a password message, containing the updated password, such that the updated password can be ascertained only by using the password,

a processor unit at the second computer to use the password to ascertain the updated password from the password message, and

a memory at the second computer to store the updated password.

25. (NEW) The system as claimed in claim 22, wherein there are a plurality of first computers, each of which has a password in common with the second computer, the password in each case being unique for the communication link between the respective first computer and the second computer.

26. (NEW) The system as claimed in claim 25, wherein there are a plurality of second computers, each of which has a password in common with each first computer, the password in each case being unique for the communication link between the respective second computer and the respective first computer.

27. (NEW) At least one computer readable medium storing at least one program for controlling at least one computer to perform a method comprising:

receiving at the second computer a service request message transmitted by the first computer over a communication link existing between the first computer and the second computer, the service request message containing the password, and being used to request provision of a service;

checking, at the second computer, whether the password contained in the service request message is valid for the first computer;

if the password is valid, providing the service;

if the password is invalid, transmitting from the second computer to the first computer an update message to request that the password be updated; and

forming an updated password.

28. (NEW) The at least one computer readable medium as claimed in claim 27, wherein after the updated password is formed, the service request message transmitted by the first computer to the second computer contains the updated password and the second computer checks whether the updated password is valid.

29. (NEW) The at least one computer readable medium as claimed in claim 27, wherein the updated password is formed in the following manner:

the first computer transmits to the second computer a password message containing the updated password, such that the updated password can be ascertained only by using the password,

the second computer uses the password to ascertain the updated password from the password message, and the second computer stores the updated password.

30. (NEW) The at least one computer readable medium as claimed in claim 29, wherein the password message contains the updated password in an encrypted form, the key for encrypting the updated password being formed on the basis of the password.

31. (NEW) The at least one computer readable medium as claimed in claim 30, wherein the key is formed by stringing together the password a number of times.

32. (NEW) The at least one computer readable medium as claimed in claim 29, wherein the second computer transmits an acknowledgment message to acknowledge the use of the updated password within the context of the communication link.

33. (NEW) The at least one computer readable medium as claimed in claim 27, wherein before the second computer checks whether the password is valid, the second computer authenticates the first computer using an authentication token for the first computer, which is contained in the service request message.

34. (NEW) The at least one computer readable medium as claimed in claim 27, wherein the check to determine whether the password contained in the service request message

is valid is performed using a monitor database indicating whether the second computer has previously transmitted an update message to the first computer.

35. (NEW) The at least one computer readable medium as claimed in claim 27, wherein

the service request message contains a statement relating to integrity protection,

the second computer checks the received service request message for its integrity,

the password is checked only if the integrity of the service request message is ensured, and

if the integrity of the service request message is not ensured the requested service is refused.

REMARKS

This Preliminary Amendment is submitted to improve the form of the specification as originally-filed. It is respectfully requested that this Preliminary Amendment be entered in the above-referenced application.

In accordance with the foregoing, claims 1-12 have been canceled and claims 13-35 have been added. Claims 13-25 are pending and are under consideration.

A substitute specification is also being filed herewith. The substitute specification is accompanied by a marked-up copy of the original specification. No new matter has been added.

If there are any questions regarding these matters, such questions can be addressed by telephone to the undersigned. Otherwise, an early action on the merits is respectfully solicited.

If any further fees are required in connection with the filing of this Preliminary Amendment, please charge same to our Deposit Account No. 19-3935.

Respectfully submitted,

STAAS & HALSEY LLP

By: ______________________
Mark J. Henry
Registration No. 36,162

700 Eleventh Street, N.W.
Suite 500
Washington, D.C. 20001
(202) 434-1500

Date: March 30, 2001

SUBSTITUTE SPECIFICATION

TITLE OF THE INVENTION

METHOD AND SYSTEM FOR UPDATING A PASSWORD

BACKGROUND OF THE INVENTION

The invention relates to a method and a system for updating a password.

Reference (1) discloses a method and system such that, if a user wants to use the system, the user is asked to enter a password into the system. Once the password has been entered by the user, the system uses a database to check whether or not an entered password is a valid password for the user.

The system's database stores a list containing permissible users of the system. Each user is allocated a respective password which is stored and has the entered password compared with it. Each password is also allocated a time statement. The time statement is used to indicate the period of time for which the password will be valid. If the period of time has elapsed, then the stored password becomes invalid, and the user is asked to update the password if he wants to use the system.

The determination of whether the respective password is up to date, is made, to a certain extent, on the basis of the respective period of time, which ensures that the system has a higher level of protection against misuse or unauthorized ascertainment of a password. Reference (1) also discloses that the stated password can be stored in the database in scrambled form (encrypted or formed using a one-way hash function). Reference (1) also discloses that the stated password can be transported in scrambled form via a communication link. An example of this is the Domain Logon in Windows NT. However, the time for changing the password is limited to the time of the login procedure.

Reference (2) discloses a communication standard, the H.235 Standard, in which boundary conditions, in particular message formats, can be exchanged between interconnected computers within the scope of multimedia communication.

The computers can be connected to one another logically or permanently.

A disadvantage of the methods disclosed in reference (2) is, in particular, that only static passwords can be used for a user. In this case, there is a relatively high likelihood of passwords stored in the computers being able to be ascertained and misused at some point in time by an unauthorized third party, a hacker. Therefore, the protection of the individual computers is no longer ensured.

Reference (3) discloses another communication standard, the H.225 Standard.

Reference (4) describes the so-called Abstract Syntax Notation 1 (ASN.1), which is used to define the format of a message within the context of the standards known from references (2) and (3).

An overview of protocols for updating cryptographic keys can be found in reference (5).

Particularly in the case of a large communication network having a multiplicity of interconnected computers, for example the Internet, the situation described above presents a high risk.

SUMMARY OF THE INVENTION

In response to the difficulties and problems of specifying a method and a system for updating a password between two interconnected computers, the present inventors propose a new method and a new system.

The method for updating a password between a first computer and a second computer has the following steps:

a) the second computer receives a service request message transmitted by the first computer over a communication link existing between the first computer and the second computer, the service request message containing the password,

b) the service request message from the first computer is used to request provision of a service,

c) the second computer checks whether the password contained in the service request message is valid for the first computer,

d) if the password is valid, the service is provided,

e) if the password is invalid, the second computer transmits to the first computer an update message which is used to request that the password be updated, and

f) the first computer and/or the second computer form an updated password which is subsequently used as the password within the context of the communication link.

The system has at least one first computer and at least one second computer for updating a password between the computers,

the first computer and the second computer each having a processor which is set up such that the following steps can be carried out:

a) the second computer receives a service request message transmitted by the first computer over a communication link existing between the first computer and the second computer, the service request message containing the password,

b) the service request message from the first computer is used to request provision of a service,

c) the second computer checks whether the password contained in the service request message is valid for the first computer,

d) if the password is valid, the service is provided,

e) if the password is invalid, the second computer transmits to the first computer an update message which is used to request that the password be updated, and

f) the first computer and/or the second computer form an updated password which is subsequently used as the password within the context of the communication link.

According to one aspect of the invention, it may be possible to update a password between two computers during a communication link existing between the two computers. The second computer can distinctly force the first computer into having to update the password when the first computer is requesting a service from the second computer. The second computer thus ensures that the passwords are up to date, which increases the protection for communication between the computers.

The developments described below apply both to the method and to the system; in the case of the development of the system, the respective processors in the computers are set up such that the development can be implemented.

In one development, the updated password is formed in the following manner:

a) the first computer transmits to the second computer a password message, containing the updated password, such that the updated password can be ascertained only by using the password,

b) the second computer uses the password to ascertain the updated password from the password message,

c) the second computer stores the updated password.

The second computer can transmit an acknowledgement message which is used to acknowledge the use of the updated password within the context of the communication link.

At the beginning of the method, the first computer is preferably authenticated by the second computer using an authentication token for the first computer, which is contained in the service request message. This increases the level of protection for the respective communication link.

In another refinement, the check to determine whether the password contained in the service request message is valid for the first computer is performed using a monitor database indicating for the first computer whether the second computer has already transmitted an update message to the first computer previously. This simplification makes the method faster to carry out, since a considerable computation time saving is obtained for the check.

The service request message preferably contains a statement relating to the integrity protection for the service request message, said statement being used by the second computer to check the received service request message for its integrity. The method is carried out only if the integrity of the service request message is ensured; otherwise, the requested service is refused. This further increases the level of protection for the respective communication link.

The password message contains the updated password preferably in encrypted form, the key for encrypting the updated password being formed on the basis of the password. This development creates a connection between the "old" password and the updated password. With the connection, perhaps only the owner of the password is actually able to ascertain the updated password. This improves the protection for the updated password when it is transmitted.

The key is preferably formed by stringing together the password a number of times.

Preferably, a plurality of first computers each have a password in common with the second computer, the password in each case being unique for the communication link between the respective first computer and the second computer. This allows for the method and system to be used very well in a large communication network in which a server, the second computer, offers a plurality of clients, the first computers, services over the communication network.

In addition, a plurality of second computers can be provided which each have a password in common with each first computer, the password in each case being unique for the communication link between the respective second computer and the respective first computer.

BRIEF DESCRIPTION OF THE DRAWINGS

These and other objects and advantages of the present invention will become more apparent and more readily appreciated from the following description of the preferred embodiments, taken in conjunction with the accompanying drawings of which:

Figure 1 shows a flowchart showing the method steps of the illustrative embodiment; and

Figure 2 shows a sketch showing computers which are connected to one another via a communication network.

DESCRIPTION OF THE PREFERRED EMBODIMENTS

Reference will now be made in detail to the preferred embodiments of the present invention, examples of which are illustrated in the accompanying drawings, wherein like reference numerals refer to like elements throughout.

Figure 2 shows a first computer 200 having a memory 202 and a processor 203 which are respectively connected to one another and to an input/output interface 201 via a bus 204.

The input/output interface 201 is used to connect the first computer 200 to a screen 205, to a keyboard 206 and to a computer mouse 207.

In addition, the first computer 200 is connected to other computers 210, 220, 230, 240 and 250 via a communication network 260, in the example an ISDN network (Integrated Services Digital Network).

The first memory 200 stores a database 208.

The other computers 210, 220, 230, 240 and 250 likewise have a respective processor 213, 223, 233, 243 and 253 and a respective memory 212, 222, 232, 242 and 252. The processor 213, 223, 233, 243 and 253 and the memory 212, 222, 232, 242 and 252 are respectively connected to the communication network 260 via a respective bus 214, 224, 234, 244 and 254 via an input/output interface 211, 221, 231, 241 and 251. In addition, the other computers 210, 220, 230, 240 and 250 are respectively connected to a screen 215, 225, 235, 245 and 255 and to a keyboard 216, 226, 236, 246 and 256 and to a computer mouse 217, 227, 237, 247 and 257.

Between the computers 200, 210, 220, 230, 240 and 250, the communication, i.e. protected interchange of multimedia data, takes place on the basis of the H.235 Standard, as described in reference (2).

The first computer 200 is in the form of a server and provides various services for the other computers 210, 220, 230, 240 and 250.

It is subsequently assumed that a second computer 210 wants to use a service from the first computer 200.

At the beginning of the method, a communication link is set up between the second computer 210 and the first computer 200 on the basis of the methods described in references

(2) and (3). Once the communication link has been initialized, a logical connection exists between the second computer 210 and the first computer 200, i.e. the communication link has an associated logical channel which is uniquely identifiable. The logical channel is used to interchange messages 270, 280 between the computers 200, 210, 220, 230, 240, 250.

If the communication link has been set up, the second computer 210 can use a service from the first computer 200, in this case a database query for a database 208 stored in the memory 202 of the first computer 200. The text below describes the method which is carried out when the second computer 210 wishes to ascertain from the first computer 200 data from the latter's database 208.

A user of the second computer 210 enters the desired criteria for the database query into the second computer 210. The second computer 210 forms a service request message 101 (step 100) containing the criteria for the database query (cf. Figure 1).

The service request message 101 also contains the following variables:

- an authentication token permitting the second computer 210 to be authenticated by the first computer 200; the authentication token permits the password to be presented in a different form (for example in encrypted form or formed using a one-way hash function as one-way hash value);
- an H.235 address used to uniquely identify the first computer 200;
- a stated password PW for the user of the second computer 210.

For each other computer 210, 220, 230, 240 and 250, the first computer 200 stores a password associated with the respective computer 210, 220, 230, 240 and 250. If a service request message 101 formed by another computer 210, 220, 230, 240 and 250 contains a stated password which is the same as the stored password for the other computer 210, 220, 230, 240 and 250, then the requested service is granted to the user, i.e. is implemented by the first computer 200.

The password has a respective associated first time statement t1, used to indicate the time at which the password has been formed. The password also has a respective associated second time statement t2, used to indicate the period of time for which the password is valid.

The service request message 101 is transmitted from the second computer 210 to the first computer 200 (step 102).

Once the service request message 101 has been received in the first computer 200 (step 103), the second computer 210 is authenticated using the authentication token in the service request message 101 (step 104).

When the second computer 210 has been positively authenticated, the stated password PW is ascertained from the authentication token in the service request message 101 in a further step (step 105), and the stated password is compared with that password stored in the first computer 200 which is associated with the second computer 200 (step 106).

If authentication is negative, the service request message 101 is discarded (step 110), and the requested service is not implemented.

If the stated password PW and the password associated with the second computer 200 match, then a check is carried out to determine whether the password is valid (step 107). This is done by ascertaining a current time t3 at which the service request message 101 has been received by the first computer 200.

If the stated password PW and the password associated with the second computer 200 do not match, then the service request message 101 is discarded (step 115), and the requested service is not implemented.

A check is carried out to determine whether the current time t3 is less than or equal to the sum of the first time statement t1 and the second time statement t2, that is to say whether the following rule (1) is true:

$$t3 \leq t1 + t2. \qquad (1)$$

If rule (1) is satisfied, then the stated password corresponds to the password, and the password is still valid.

In this case, the service requested using the service request 101, that is to say the database query, is implemented by the first computer 200 (step 108), and the result of the database query is transmitted in a formed result message 116 (step 109) to the second computer 210 (step 110), in which the result of the database query is processed further (step 111).

If rule (1) is not satisfied, then, although the authentication which has taken place authorizes the second computer 210 to request the service, in principle, the password associated with the second computer 210 is no longer valid.

In a further step (step 120), if a password is invalid, the first computer 200 forms an update message 121 and transmits it to the second computer 210 (step 122), said update message being used to request that the password be updated. In addition, the first computer 200 sets a bit (monitor value) to a first value in a monitor database, said value being used to indicate that the respective password is invalid and the appropriate update message 121 has been transmitted to the second computer 210.

When the update message 121 has been received (step 123), the second computer forms an updated password aPW (step 124).

If the second computer 210 does not keep to the prescribed procedure and generates a new service request without changing the password, then the first computer 200 is able to establish this after authentication of the second computer 210 and checking of the monitor value. If the monitor value has been set to the first value, the method can be terminated (step 131).

The updated password aPW is encrypted symmetrically on the basis of the Data Encryption Standard (DES). The key used to encrypt the updated password aPW is the password PW, which is also known and stored in the second computer 210.

The encrypted updated password aPW is transmitted to the first computer (step 127) in a password message 125 formed by the second computer 210 (step 126).

The password message 125 contains an integrity statement which can be used to check the integrity of the password message 125.

Once the password message 125 has been received (step 128), the integrity of the password message (125) is checked (step 129).

If the integrity check is negative, the password message 125 is discarded (step 130), and the method is terminated (step 131).

If the integrity check is positive, the first computer 200 ascertains the encrypted updated password aPW (step 132), and the updated password aPW is decrypted (step 133).

In a further step, the ascertained updated password aPW is stored as the new password for the second computer 210 (step 134). In addition, the first computer 200 sets the appropriate monitor value in the monitor database to a second value, which is used to indicate that the respective password is valid.

Next, the first computer 200 forms an acknowledgment message 135 (step 136) and transmits it to the second computer 210 (step 137), and said acknowledgment message is received by the second computer 210 (step 138). The acknowledgment message 135 is used to acknowledge to the second computer 210 the further use of the updated password aPW within the context of the communication link.

In addition, the first computer 200 provides the service (step 108), forms the result message 116 (step 109) and transmits the result message 116 to the second computer 210 (step 110). In the second computer 210, the result message 116 is processed further (step 111).

The first computer 200 also sets the appropriate bit in the monitor database to a second value, which is used to indicate that the respective password is valid.

When another service request message is received, in each case after receipt thereof, the first computer 200 uses the monitor database to check whether or not the respective password is valid. This allows the password to be checked very quickly.

The messages used within the context of this method may be coded for example, on the basis of the H.225.0 Standard, as is described in reference (3).

To define the format (described below) of the individual messages, the Abstract Syntax

Notation 1 (ASN.1), for example, described in reference (4) may be used.

The messages are coded as a NonStandardMessage provided in reference (3), as described below:

```
NonStandardMessage ::= SEQUENCE
{
      requestSeqNum           RequestSeqNum,
      nonStandardData   NonStandardParameter,
      ...
      tokens                  SEQUENCE OF ClearToken OPTIONAL,
      cryptoTokens            SEQUENCE OF CryptoH323Token OPTIONAL,
      integrityCheckValue     ICV OPTIONAL
}


NonStandardParameter ::= SEQUENCE
{
      nonStandardIdentifier   NonStandardIdentifier,
      data                          OCTET STRING
}


NonStandardIdentifier ::= CHOICE
{
      object                  OBJECT IDENTIFIER,
      h221NonStandard   H221NonStandard,
      ...
}


data ::= SEQUENCE
{
      alias             GatekeeperIdentifier,
      confirm                 boolean,

      -- optionally for the provision of integrity
      rejectReason            PWUpdateRejectReason   OPTIONAL,
      hash_algorithm          NonIsoIntegrityMechanism     OPTIONAL,
      token             HASHED OPTIONAL,
                              -- < alias, confirmation, new password>

      ...
}


PWUpdateRejectReason ::= CHOICE
{
      notregistered           NULL, -- keep the old password
      pw_wrong                NULL, -- keep the old password
      pw_old                  NULL, -- keep the old password
      ...
}
```

```
NonIsoIntegrityMechanism ::= CHOICE
(     -- HMAC mechanism used, no truncation, tagging may bei dem
necessary!
      hMAC-MD5                  NULL,
      hMAC-iso10118-2-s EncryptIntAlg,
      -- according to ISO/IEC 10118-2 using
      -- EncryptIntAlg as core block encryption algorithm
      -- (short MAC)
      hMAC-iso10118-2-1 EncryptIntAlg,
      -- according to ISO/IEC 10118-2 using
      -- EncryptIntAlg as core block encryption algorithm
      -- (long MAC)
      hMAC-iso10118-3   OBJECT IDENTIFIER,
      -- according to ISO/IEC 10118-3 using
      -- OID as hash function (OID is SHA-1, RIPE-MD160,
      -- RIPE-MD128)
      ...
}


EncryptIntAlg ::= CHOICE
{     -- core encryption algorithms for RAS message integrity
      nonStandard       NonStandardParameter,
      isoAlgorithm            OBJECT IDENTIFIER,      -- defined in
ISO/IEC 9979
      ...
}


AliasAddress ::= CHOICE
{
      e164        IA5String (SIZE (1..128)) (FROM („0123456789#*,")),
      h323-ID     BMPString (SIZE (1..256)),
                  -- Basic ISO/IEC 10646-1 (Unicode)
      ...,
      url-ID      IA5String (SIZE (1..512)),
                  -- URL style address
      transportID TransportAddress,
      email-ID    IA5String (SIZE (1..512)),
                  -- rfc822-compliant email address
      partyNumber PartyNumber
}
```

A few alternatives to the illustrative embodiment described above are presented below:

The type of integrity protection is, in principle, arbitrary, as is the encryption algorithm for encrypting the updated password.

Providing the messages as nonstandard messages or nonstandard data field is not absolutely necessary. The messages may also be presented using protocol fields or messages which are to be newly defined, in the standards known from references (2) and (3).

The method and the system are also not limited to the standards known from references (2) and (3).

The service request message and/or the update message and/or the password message and/or the acknowledgment message can be formed separately as independent messages and can be transmitted separately between the computers which are involved. In addition, in one variant, the respective message can be transmitted between the computers involved together with other messages on the basis of the so-called "piggyback" principle.

By transmitting an update request to the first computer, the second computer can also request that the first computer form a new password. On a similar basis to the above comments, the second computer can use a monitor database stored therein and the appropriate monitor value to check whether the first computer has satisfied its request to change the password. In the negative instance, the second computer can abort the communication and terminate the method.

The following publications are cited in this document:

(1) Microsoft Developer Network Library, Questions 151082 S7D6D, S7590, S759E, S5970, Microsoft Press, July 1998, available on September 29, 1998 on the Internet at the following address:
http://msdn.microsoft.com/developer/

(2) International Telecommunication Union, Draft ITU-T Recommendation H.235, Line Transmission of Non-Telephone Signals, Security and Encryption for H Series (H.323 and Other H.245 Based) Multimedia Terminals), Version 1, Section 10.3.2, September 1997

(3) International Telecommunication Union, Draft ITU-T Recommendation H.225.0, Line Transmission of Non-Telephone Signals, Call Signaling Protocols and Media Stream Packetization for Packet Based Multimedia Communications Systems, Version 2, Sections 7.6 and 7.16, March 1997

(4) International Telecommunication Union, X.680 - X.683: OSI NETWORKING AND SYSTEMS ASPECTS - ABSTRACT SYNTAX NOTATION ONE (ASN.1), July 1994

(5) A. J. Menezes et al., Handbook of Applied Cryptography, CRC Press, New York, pp. 497 - 504, 1997, ISDN 0-8493-8523-7

SUBSTITUTE ABSTRACT

A password is updated between a first computer and a second computer, where the second computer receives a service request message transmitted by the first computer over a communication link existing between the first computer and the second computer, the service request message containing the password, the service request message from the first computer is used to request provision of a service, the second computer checks whether the password contained in the service request message is valid for the first computer, if the password is valid, the service is provided, if the password is invalid, the second computer transmits to the first computer an update message which is used to request that the password be updated, and the first computer forms an updated password which is subsequently used as the password within the context of the communication link.

Description

Method and arrangement for updating a password

The invention relates to a method and an arrangement for updating a password.

[1] discloses such a method and such an arrangement.

In such an arrangement, if a user wants to use this arrangement, the user is asked to enter a password into the arrangement. Once the password has been entered by the user, the arrangement uses a database to check whether or not an entered password is a valid password for the user.

The arrangement's database stores a list containing permissible users of the arrangement. Each user is allocated a respective password which is stored and has the entered password compared with it. Each password is also allocated a time statement. The time statement is used to indicate the period of time for which the password will be valid. If the period of time has elapsed, then the stored password becomes invalid, and the user is asked to update the password if he wants to use the arrangement.

This means that the respective password is up to date, to a certain extent, on the basis of the respective period of time, which ensures that the arrangement has a higher level of protection against misuse or unauthorized ascertainment of a password. [1] also discloses that the stated password can be stored in the database in scrambled form (encrypted or formed using a one-way hash function). [1] also discloses that the stated password can be transported in scrambled form via a communication link. An example of this is the Domain Logon in Windows NT. However, the time for changing the password is limited to the time of the login procedure.

[2] discloses a communication standard, the H.235 Standard, in which boundary conditions, in particular message formats, can be exchanged between interconnected computers within the scope of multimedia communication.

The computers can be connected to one another logically or permanently.

A disadvantage of the methods disclosed in [2] is, in particular, that only static passwords can be used for a user, which means that there is a relatively high likelihood of passwords stored in the computers being able to be ascertained and misused at some point in time by an unauthorized third party, a hacker, which means that the protection of the individual computers is no longer ensured.

[3] discloses another communication standard, the H.225 Standard.

[4] describes the so-called Abstract Syntax Notation 1 (ASN.1), which is used to define the format of a message within the context of the standards known from [2] and [3].

An overview of protocols for updating cryptographic keys can be found in [5].

Particularly in the case of a large communication network having a multiplicity of interconnected computers, for example the Internet, the situation described above presents a high risk.

The invention is thus based on the problem of specifying a method and an arrangement for updating a password between two interconnected computers.

The problem is solved by the arrangement and the method having the features in accordance with the independent claims.

A method for updating a password between a first computer and a second computer has the following steps:

a) the second computer receives a service request message transmitted by the first computer over a communication link existing between the first computer and the second computer, the service request message containing the password,

b) the service request message from the first computer is used to request provision of a service,

c) the second computer checks whether the password contained in the service request message is valid for the first computer,

d) if the password is valid, the service is provided,

e) if the password is invalid, the second computer transmits to the first computer an update message which is used to request that the password be updated, and

f) the first computer and/or the second computer form an updated password which is subsequently used as the password within the context of the communication link.

An arrangement has at least one first computer and at least one second computer for updating a password between the computers,

the first computer and the second computer each having a processor which is set up such that the following steps can be carried out:

a) the second computer receives a service request message transmitted by the first computer over a communication link existing between the first computer and the second computer, the service request message containing the password,

b) the service request message from the first computer is used to request provision of a service,

c) the second computer checks whether the password contained in the service request message is valid for the first computer,

d) if the password is valid, the service is provided,

e) if the password is invalid, the second computer transmits to the first computer an update message which is used to request that the password be updated, and

f) the first computer and/or the second computer form an updated password which is subsequently used as the password within the context of the communication link.

The invention makes it possible to update a password between two computers during a communication link existing between the two computers. The second computer can distinctly force the first computer into having to update the password when the first computer is requesting a service from the second computer. This means that the second computer ensures that the passwords are up to date, which increases the protection for communication between the computers.

Preferred developments of the invention can be found in the dependent claims.

The developments described below apply both to the method and to the arrangement; in the case of the development of the arrangement, the respective processors in the computers are set up such that the development can be implemented.

In one development, the updated password is formed in the following manner:

a) the first computer transmits to the second computer a password message, containing the updated password, such that the updated password can be ascertained only by using the password,

b) the second computer uses the password to ascertain the updated password from the password message,

c) the second computer stores the updated password.

The second computer can transmit an acknowledgement message which is used to acknowledge the use of the updated password within the context of the communication link.

At the beginning of the method, the first computer is preferably authenticated by the second computer using an authentication token for the first computer, which is contained in the service request message. This increases the level of protection for the respective communication link.

In another refinement, the check to determine whether the password contained in the service request message is valid for the first computer is performed using a monitor database indicating for the first computer whether the second computer has already transmitted an update message to the first computer previously. This simplification makes the method faster to carry out, since a considerable computation time saving is obtained for the check.

The service request message preferably contains a statement relating to the integrity protection for the service request message, said statement being used by the second computer to check the received service request message for its integrity. The method is carried out only if the integrity of the service request message is ensured; otherwise, the requested service is refused. This further increases the level of protection for the respective communication link.

The password message contains the updated password preferably in encrypted form, the key for encrypting the updated password being formed on the basis of the password. This development creates a connection between the "old" password and the updated password, which means that only the owner of the password is actually able to ascertain the updated password. This improves the protection for the updated password when it is transmitted.

The key is preferably formed by stringing together the password a number of times.

Preferably, a plurality of first computers is provided which each have a password in common with the second computer, the password in each case being unique for the communication link between the respective first computer and the second computer. This means that the invention can be used very well in a large communication network in which a server, the second computer, offers a plurality of clients, the first computers, services over the communication network.

In addition, a plurality of second computers can be provided which each have a password in common with each first computer, the password in each case being unique for the communication link between the respective second computer and the respective first computer.

An illustrative embodiment of the invention is shown in the figures and is explained in more detail below:

In the figures

Figure 1 shows a flowchart showing the method steps of the illustrative embodiment;

Figure 2 shows a sketch showing computers which are connected to one another via a communication network.

Figure 2 shows a first computer 200 having a memory 202 and a processor 203 which are respectively connected to one another and to an input/output interface 201 via a bus 204.

The input/output interface 201 is used to connect the first computer 200 to a screen 205, to a keyboard 206 and to a computer mouse 207.

In addition, the first computer 200 is connected to other computers 210, 220, 230, 240 and 250 via a communication network 260, in the example an ISDN network (Integrated Services Digital Network).

The first memory 200 stores a database 208.

The other computers 210, 220, 230, 240 and 250 likewise have a respective processor 213, 223, 233, 243 and 253 and a respective memory 212, 222, 232, 242 and 252. The processor 213, 223, 233, 243 and 253 and the memory 212, 222, 232, 242 and 252 are respectively connected to the communication network 260 via a respective bus 214, 224, 234, 244 and 254 via an input/output interface 211, 221, 231, 241 and 251. In addition, the other computers 210, 220, 230, 240 and 250 are respectively connected to a screen 215, 225, 235, 245 and 255 and to a keyboard 216, 226, 236, 246 and 256 and to a computer mouse 217, 227, 237, 247 and 257.

Between the computers 200, 210, 220, 230, 240 and 250, the communication, i.e. protected interchange of multimedia data, takes place on the basis of the H.235 Standard, as described in [2].

The first computer 200 is in the form of a server and provides various services for the other computers 210, 220, 230, 240 and 250.

It is subsequently assumed that a second computer 210 wants to use a service from the first computer 200.

At the beginning of the method, a communication link is set up between the second computer 210 and the first computer 200 on the basis of the methods described in [2] and [3]. Once the communication link has been initialized, a logical connection exists between the second computer 210 and the first computer 200, i.e. the communication link has an associated logical channel which is uniquely identifiable. The logical channel is used to interchange messages 270, 280 between the computers 200, 210, 220, 230, 240, 250.

If the communication link has been set up, the second computer 210 can use a service from the first computer 200, in this case a database query for a database 208 stored in the first computer 200.

The text below describes the method which is carried out when the second computer 210 wishes to ascertain from the first computer 200 data from the latter's database 208.

A user of the second computer 210 enters the desired criteria for the database query into the second computer 210. The second computer 210 forms a service request message 101 (step 100) containing the criteria for the database query (cf. **Figure 1**).

The service request message 101 also contains the following variables:

- an authentication token permitting the second computer 210 to be authenticated by the first computer 200; the authentication token permits the password to be presented in a different form (for example in encrypted form or formed using a one-way hash function as one-way hash value);
- an H.235 address used to uniquely identify the first computer 200;
- a stated password PW for the user of the second computer 210.

For each other computer 210, 220, 230, 240 and 250, the first computer 200 stores a password associated with the respective computer 210, 220, 230, 240 and 250. If a service request message 101 formed by another computer 210, 220, 230, 240 and 250 contains a stated password which is the same as the stored password for the other computer 210, 220, 230, 240 and 250, then the requested service is granted to the user, i.e. is implemented by the first computer 200.

The password has a respective associated first time statement t1, used to indicate the time at which the password has been formed. The password also has a respective associated second time statement t2, used to indicate the period of time for which the password is valid.

The service request message 101 is transmitted from the second computer 210 to the first computer 200 (step 102).

Once the service request message 101 has been received in the first computer 200 (step 103), the second computer 210 is authenticated using the authentication token in the service request message 101 (step 104).

When the second computer 210 has been positively authenticated, the stated password PW is ascertained from the authentication token in the service request message 101 in a further step (step 105), and the stated password is compared with that password stored in the first computer 200 which is associated with the second computer 200 (step 106).

If authentication is negative, the service request message 101 is discarded (step 110), and the requested service is not implemented.

If the stated password PW and the password associated with the second computer 200 match, then a check is carried out to determine whether the password is valid (step 107). This is done by ascertaining a current time t3 at which the service request message 101 has been received by the first computer 200.

If the stated password PW and the password associated with the second computer 200 do not match, then the service request message 101 is discarded (step 115), and the requested service is not implemented.

A check is carried out to determine whether the current time t3 is less than or equal to the sum of the first time statement t1 and the second time statement t2, that is to say whether the following is true:

$$t3 \leq t1 + t2. \qquad (1)$$

If rule (1) is satisfied, this means that the stated password corresponds to the password, and the password is still valid.

In this case, the service requested using the service request 101, that is to say the database query, is implemented by the first computer 200 (step 108), and the result of the database query is transmitted in a formed result message 116 (step 109) to the second computer 210 (step 110), in which the result of the database query is processed further (step 111).

If rule (1) is not satisfied, this means that, although the authentication which has taken place authorizes the second computer 210 to request the service, in principle, the password associated with the second computer 210 is no longer valid.

In a further step (step 120), if a password is invalid, the first computer 200 forms an update message 121 and transmits it to the second computer 210 (step 122), said update message being used to request that the password be updated. In addition, the first computer 200 sets a bit (monitor value) to a first value in a monitor database, said value being used to indicate that the respective password is invalid and the appropriate update message 121 has been transmitted to the second computer 210.

When the update message 121 has been received (step 123), the second computer forms an updated password aPW (step 124).

If the second computer 210 does not keep to the prescribed procedure and generates a new service request without changing the password, then the first computer 200 is able to establish this after authentication of the second computer 210 and checking of the monitor value. If the monitor value has been set to the first value, the method can be terminated (step 131).

The updated password aPW is encrypted symmetrically on the basis of the Data Encryption Standard (DES). The key used to encrypt the updated password aPW is the password PW, which is also known and stored in the second computer 210.

The encrypted updated password aPW is transmitted to the first computer (step 127) in a password message 125 formed by the second computer 210 (step 126).

The password message 125 contains an integrity statement which can be used to check the integrity of the password message 125.

Once the password message 125 has been received (step 128), the integrity of the password message (125) is checked (step 129).

If the integrity check is negative, the password message 125 is discarded (step 130), and the method is terminated (step 131).

If the integrity check is positive, the first computer 200 ascertains the encrypted updated password aPW (step 132), and the updated password aPW is decrypted (step 133).

In a further step, the ascertained updated password aPW is stored as the new password for the second computer

210 (step 134). In addition, the first computer 200 sets the appropriate monitor value in the monitor database to a second value, which is used to indicate that the respective password is valid.

Next, the first computer 200 forms an acknowledgement message 135 (step 136) and transmits it to the second computer 210 (step 137), and said acknowledgement message is received by the second computer 210 (step 138). The acknowledgement message 135 is used to acknowledge to the second computer 210 the further use of the updated password aPW within the context of the communication link.

In addition, the first computer 200 provides the service (step 108), forms the result message 116 (step 109) and transmits the result message 116 to the second computer 210 (step 110). In the second computer 210, the result message 116 is processed further (step 111).

The first computer 200 also sets the appropriate bit in the monitor database to a second value, which is used to indicate that the respective password is valid.

When another service request message is received, in each case after receipt thereof, the first computer 200 uses the monitor database to check whether or not the respective password is valid. This allows the password to be checked very quickly.

The messages used within the context of this method are coded on the basis of the H.225.0 Standard, as is described in [3].

To define the format (described below) of the individual messages, the Abstract Syntax Notation 1 (ASN.1) described in [4] is used.

The messages are coded as a NonStandardMessage provided in [3], as described below:

```
NonStandardMessage ::= SEQUENCE
{
      requestSeqNum            RequestSeqNum,
      nonStandardData    NonStandardParameter,
      ...
      tokens                   SEQUENCE OF ClearToken OPTIONAL,
      cryptoTokens             SEQUENCE OF CryptoH323Token OPTIONAL,
      integrityCheckValue      ICV OPTIONAL
}

NonStandardParameter ::= SEQUENCE
{
      nonStandardIdentifier    NonStandardIdentifier,
      data                            OCTET STRING
}

NonStandardIdentifier ::= CHOICE
{
      object                   OBJECT IDENTIFIER,
      h221NonStandard    H221NonStandard,
      ...
}

data ::= SEQUENCE
{
      alias              GatekeeperIdentifier,
      confirm                  boolean,

      -- optionally for the provision of integrity
      rejectReason             PWUpdateRejectReason    OPTIONAL,
      hash_algorithm           NonIsoIntegrityMechanism      OPTIONAL,
      token              HASHED OPTIONAL,
                               -- < alias, confirmation, new password>
      ...
}

PWUpdateRejectReason ::= CHOICE
{
      notregistered            NULL, -- keep the old password
      pw_wrong                 NULL, -- keep the old password
      pw_old                   NULL, -- keep the old password
      ...
}
```

```
NonIsoIntegrityMechanism ::= CHOICE
{     -- HMAC mechanism used, no truncation, tagging may bei dem
necessary!
      hMAC-MD5                NULL,
      hMAC-iso10118-2-s EncryptIntAlg,
      -- according to ISO/IEC 10118-2 using
      -- EncryptIntAlg as core block encryption algorithm
      -- (short MAC)
      hMAC-iso10118-2-1 EncryptIntAlg,
      -- according to ISO/IEC 10118-2 using
      -- EncryptIntAlg as core block encryption algorithm
      -- (long MAC)
      hMAC-iso10118-3   OBJECT IDENTIFIER,
      -- according to ISO/IEC 10118-3 using
      -- OID as hash function (OID is SHA-1, RIPE-MD160,
      -- RIPE-MD128)
      ...
}


EncryptIntAlg ::= CHOICE
{     -- core encryption algorithms for RAS message integrity
      nonStandard       NonStandardParameter,
      isoAlgorithm            OBJECT IDENTIFIER,      -- defined in
ISO/IEC 9979
      ...
}


AliasAddress ::= CHOICE
{
      e164        IA5String (SIZE (1..128)) (FROM („0123456789#*,")),
      h323-ID     BMPString (SIZE (1..256)),
                  -- Basic ISO/IEC 10646-1 (Unicode)
      ...,
      url-ID      IA5String (SIZE (1..512)),
                  -- URL style address
      transportID TransportAddress,
      email-ID    IA5String (SIZE (1..512)),
                  -- rfc822-compliant email address
      partyNumber PartyNumber
}
```

A few alternatives to the illustrative embodiment described above are presented below:

The type of integrity protection is, in principle, arbitrary, as is the encryption algorithm for encrypting the updated password.

Providing the messages as nonstandard messages or nonstandard data field is not absolutely necessary. The messages may also be presented using protocol fields or messages which are to be newly defined, in the standards known from [2] and [3].

The method and the arrangement are also not limited to the standards known from [2] and [3].

The service request message and/or the update message and/or the password message and/or the acknowledgement message can be formed separately as independent messages and can be transmitted separately between the computers which are involved. In addition, in one variant, the respective message can be transmitted between the computers involved together with other messages on the basis of the so-called "piggyback" principle.

By transmitting an update request to the first computer, the second computer can also request that the first computer form a new password. On a similar basis to the above comments, the second computer can use a monitor database stored therein and the appropriate monitor value to check whether the first computer has satisfied its request to change the password. In the negative instance, the second computer can abort the communication and terminate the method.

The following publications are cited in this document:

[1] Microsoft Developer Network Library, Questions 151082 S7D6D, S7590, S759E, S5970, Microsoft Press, July 1998, available on September 29, 1998 on the Internet at the following address: http://msdn.microsoft.com/developer/

[2] International Telecommunication Union, Draft ITU-T Recommendation H.235, Line Transmission of Non-Telephone Signals, Security and Encryption for H Series (H.323 and Other H.245 Based) Multimedia Terminals), Version 1, Section 10.3.2, September 1997

[3] International Telecommunication Union, Draft ITU-T Recommendation H.225.0, Line Transmission of Non-Telephone Signals, Call Signaling Protocols and Media Stream Packetization for Packet Based Multimedia Communications Systems, Version 2, Sections 7.6 and 7.16, March 1997

[4] International Telecommunication Union, X.680 - X.683: OSI NETWORKING AND SYSTEMS ASPECTS - ABSTRACT SYNTAX NOTATION ONE (ASN.1), July 1994

[5] A. J. Menezes et al., Handbook of Applied Cryptography, CRC Press, New York, pp. 497 - 504, 1997, ISDN 0-8493-8523-7

Patent claims

1. A method for updating a password between a first computer and a second computer,

a) in which the second computer receives a service request message transmitted by the first computer over a communication link existing between the first computer and the second computer, the service request message containing the password,

b) in which the service request message from the first computer is used to request provision of a service,

c) in which the second computer checks whether the password contained in the service request message is valid for the first computer,

d) in which, if the password is valid, the service is provided,

e) in which, if the password is invalid, the second computer transmits to the first computer an update message which is used to request that the password be updated, and

f) in which the first computer and/or the second computer form an updated password which is subsequently used as the password within the context of the communication link.

2. The method as claimed in claim 1,

in which the updated password is formed in the following manner:

a) the first computer transmits to the second computer a password message, containing the updated password, such that the updated password can be ascertained only by using the password,

b) the second computer uses the password to ascertain the updated password from the password message,

c) the second computer stores the updated password.

3. The method as claimed in claim 2,

in which the second computer transmits an acknowledgement message which is used to acknowledge the use of the updated password within the context of the communication link.

4. The method as claimed in one of claims 1 to 3,

in which, at the beginning of the method, the first computer is authenticated by the second computer using an authentication token for the first computer, which is contained in the service request message.

5. The method as claimed in one of claims 1 to 4,

in which the check to determine whether the password contained in the service request message is valid for the first computer is performed using a monitor database indicating for the first computer whether the second computer has already transmitted an update message to the first computer previously.

6. The method as claimed in one of claims 1 to 5,

a) in which the service request message contains a statement relating to integrity protection for the service request message,

b) in which the second computer checks the received service request message for its integrity,

c) in which the method is carried out only if the integrity of the service request message is ensured, and

d) otherwise, the requested service is refused.

7. The method as claimed in one of claims 2 to 6,

in which the password message contains the updated password in encrypted form, the key for encrypting the updated password being formed on the basis of the password.

8. The method as claimed in claim 7,

in which the key is formed by stringing together the password a number of times.

9. An arrangement having at least one first computer and at least one second computer for updating a password between the computers,

the first computer and the second computer each having a processor which is set up such that the following steps can be carried out:

a) the second computer receives a service request message transmitted by the first computer over a communication link existing between the first computer and the second computer, the service request message containing the password,

b) the service request message from the first computer is used to request provision of a service,

c) the second computer checks whether the password contained in the service request message is valid for the first computer,

d) if the password is valid, the service is provided,

e) if the password is invalid, the second computer transmits to the first computer an update message which is used to request that the password be updated, and

f) the first computer and/or the second computer form an updated password which is subsequently used as the password within the context of the communication link.

10. The arrangement as claimed in claim 9,

in which the processors are set up such that the updated password is formed in the following manner:

a) the first computer transmits to the second computer a password message, containing the updated password, such that the updated password can be ascertained only by using the password,

b) the second computer uses the password to ascertain the updated password from the password message,

c) the second computer stores the updated password.

11. The arrangement as claimed in claim 9 or 10,

having a plurality of first computers which each have a password in common with the second computer, the password in each case being unique for the communication link between the respective first computer and the second computer.

12. The arrangement as claimed in one of claims 9 to 11,

having a plurality of second computers which each have a password in common with each first computer, the password in each case being unique for the communication link between the respective second computer and the respective first computer.

Abstract

Method and arrangement for updating a password

A password is updated between a first computer and a second computer, where

a) the second computer receives a service request message transmitted by the first computer over a communication link existing between the first computer and the second computer, the service request message containing the password,

b) the service request message from the first computer is used to request provision of a service,

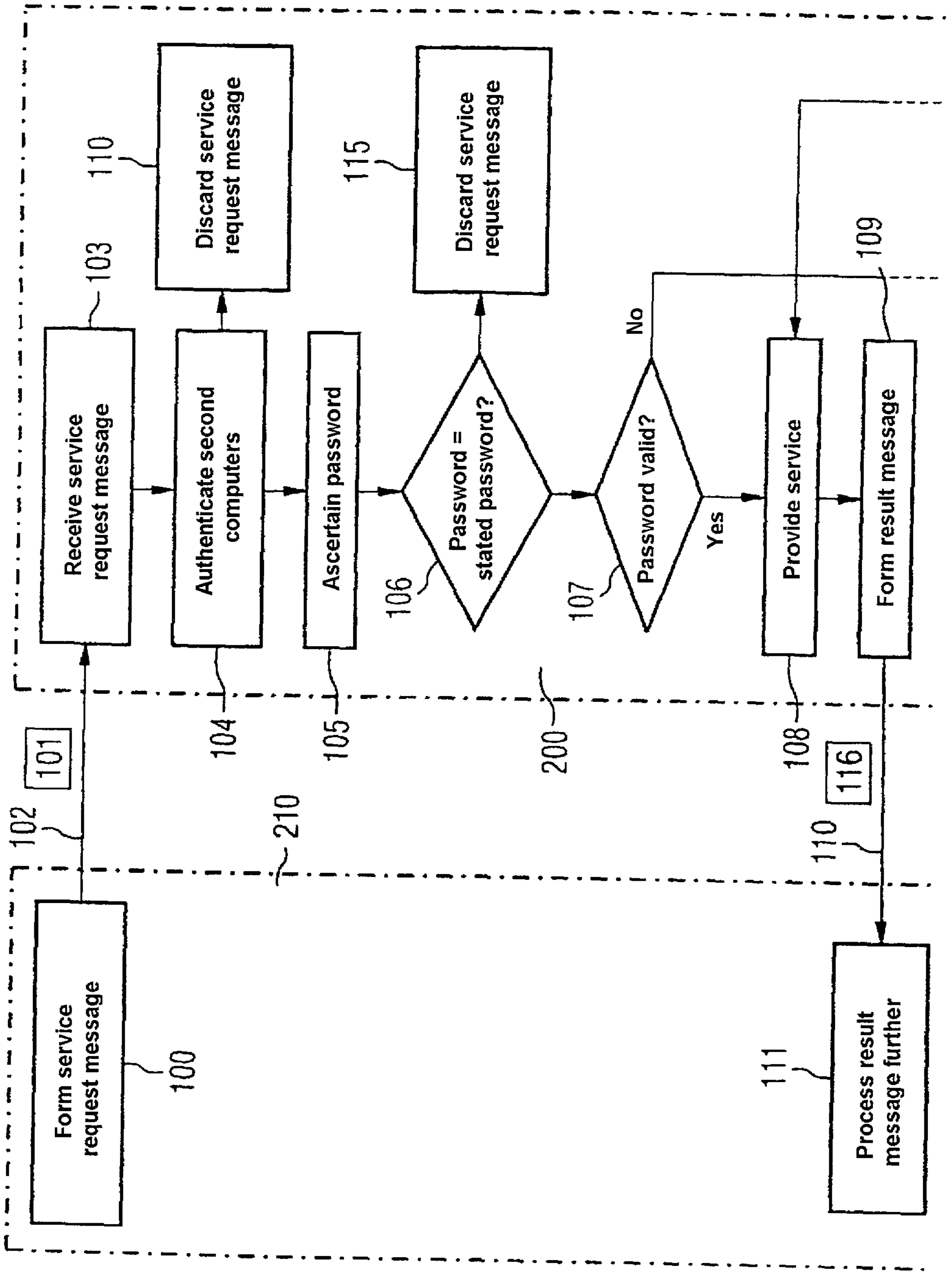
c) the second computer checks whether the password contained in the service request message is valid for the first computer,

d) if the password is valid, the service is provided,

e) if the password is invalid, the second computer transmits to the first computer an update message which is used to request that the password be updated, and

f) the first computer forms an updated password which is subsequently used as the password within the context of the communication link.

FIG 1A


Form service request message
100
102
101
Receive service request message
103
Authenticate second computers
104
Discard service request message
110
Ascertain password
105
Password = stated password?
106
Discard service request message
115
Password valid?
107
No
Yes
Provide service
108
Form result message
109
116
110
Process result message further
111
200
210

GR 98 P 2821

09/806435

FIG 1B

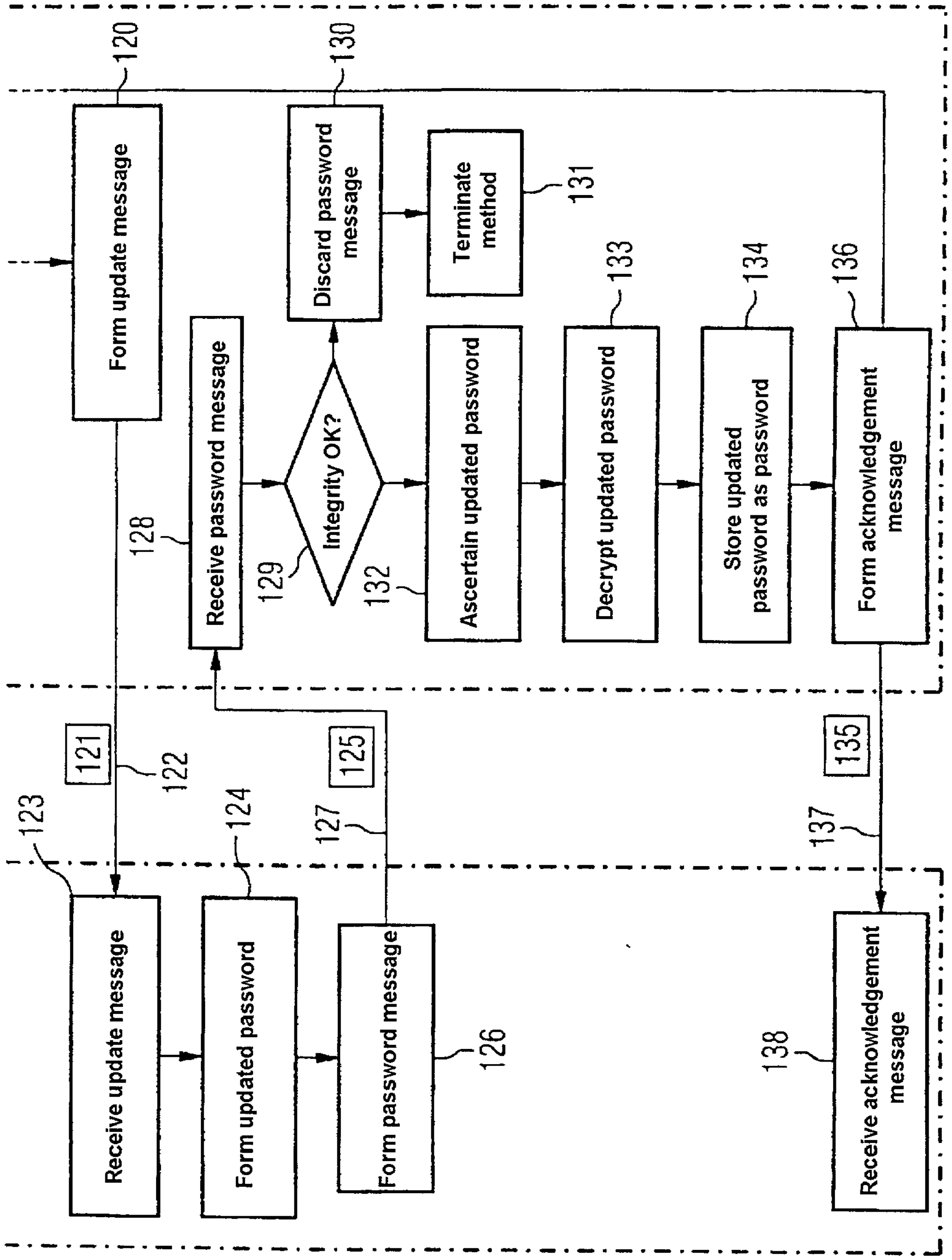
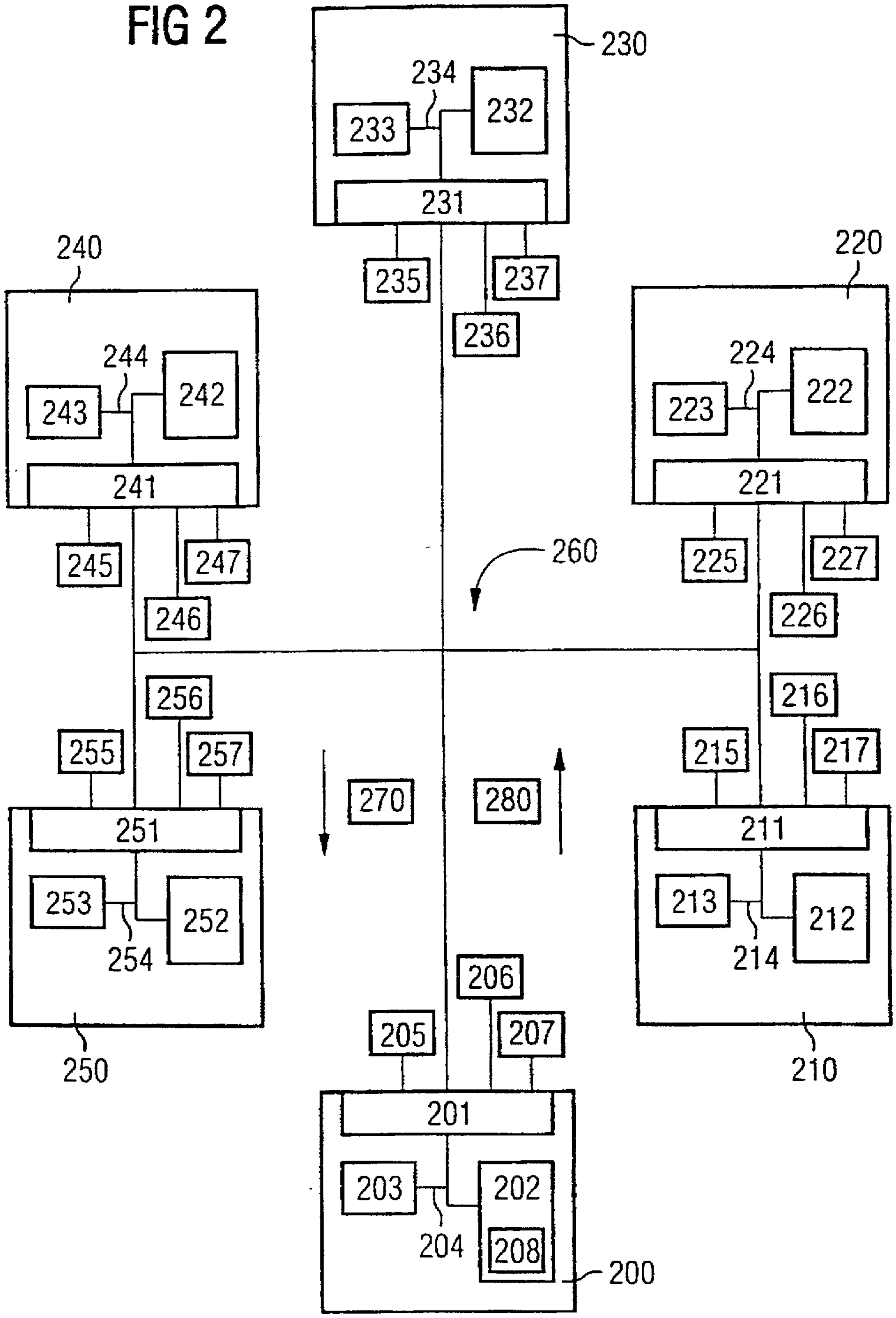


FIG 2


230
234
233
232
231
235
236
237
240
244
243
242
241
245
246
247
220
224
223
222
221
225
226
227
260
256
255
257
251
253
252
254
250
270
280
216
215
217
211
213
212
214
210
206
205
207
201
203
202
208
204
200

Declaration and Power of Attorney For Patent Application

Erklärung Für Patentanmeldungen Mit Vollmacht

German Language Declaration

Als nachstehend benannter Erfinder erkläre ich hiermit an Eides Statt:

dass mein Wohnsitz, meine Postanschrift, und meine Staatsangehörigkeit den im Nachstehenden nach meinem Namen aufgeführten Angaben entsprechen,

dass ich, nach bestem Wissen der ursprüngliche, erste und alleinige Erfinder (falls nachstehend nur ein Name angegeben ist) oder ein ursprünglicher, erster und Miterfinder (falls nachstehend mehrere Namen aufgeführt sind) des Gegenstandes bin, für den dieser Antrag gestellt wird und für den ein Patent beantragt wird für die Erfindung mit dem Titel:

Verfahren und Anordnung zur Aktualisierung eines Passwortes

deren Beschreibung

(zutreffendes ankreuzen)

□ hier beigefügt ist.

☒ am 08. September 1999 als PCT internationale Anmeldung
PCT Anmeldungsnummer PCT/DE99/02844
eingereicht wurde und am ____________________
abgeändert wurde (falls tatsächlich abgeändert).

Ich bestätige hiermit, dass ich den Inhalt der obige□n Patentanmeldung einschliesslich der Ansprüche durchgesehen und verstanden habe, die eventuell durch einen Zusatzantrag wie oben erwähnt abgeändert wurde.

Ich erkenne meine Pflicht zur Offenbarung irgendwelcher Informationen, die für die Prüfung der vorliegenden Anmeldung in Einklang mit Absatz 37, Bundesgesetzbuch, Paragraph 1.56(a) von Wichtigkeit sind, an.

Ich beanspruche hiermit ausländische Prioritätsvorteile gemäss Abschnitt 35 der Zivilprozessordnung der Vereinigten Staaten, Paragraph 119 aller unten angegebenen Auslandsanmeldungen für ein Patent oder eine Erfindersurkunde, und habe auch alle Auslandsanmeldungen für ein Patent oder eine Erfindersurkunde nachstehend gekennzeichnet, die ein Anmeldedatum haben, das vor dem Anmeldedatum der Anmeldung liegt, für die Priorität beansprucht wird.

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name,

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled

____
____

the specification of which

(check one)

□ is attached hereto.

□ was filed on ____________________ as
PCT international application
PCT Application No. ____________________
and was amended on ____________________
(if applicable)

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims as amended by any amendment referred to above.

I acknowledge the duty to disclose information which is material to the examination of this application in accordance with Title 37, Code of Federal Regulations, §1.56(a).

I hereby claim foreign priority benefits under Title 35, United States Code, §119 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

German Language Declaration

Prior foreign appplications
Priorität beansprucht

Priority Claimed

198 45 055.9 Germany 30. September 1998 ☒ Yes Ja □ No Nein
(Number) (Nummer) (Country) (Land) (Day Month Year Filed) (Tag Monat Jahr eingereicht)

(Number) (Nummer) (Country) (Land) (Day Month Year Filed) (Tag Monat Jahr eingereicht) □ Yes Ja □ No Nein

(Number) (Nummer) (Country) (Land) (Day Month Year Filed) (Tag Monat Jahr eingereicht) □ Yes Ja □ No Nein

Ich beanspruche hiermit gemäss Absatz 35 der Zivilprozessordnung der Vereinigten Staaten, Paragraph 120, den Vorzug aller unten aufgeführten Anmeldungen und falls der Gegenstand aus jedem Anspruch dieser Anmeldung nicht in einer früheren amerikanischen Patentanmeldung laut dem ersten Paragraphen des Absatzes 35 der Zivilprozeßordnung der Vereinigten Staaten, Paragraph 122 offenbart ist, erkenne ich gemäss Absatz 37, Bundesgesetzbuch, Paragraph 1.56(a) meine Pflicht zur Offenbarung von Informationen an, die zwischen dem Anmeldedatum der früheren Anmeldung und dem nationalen oder PCT internationalen Anmeldedatum dieser Anmeldung bekannt geworden sind.

I hereby claim the benefit under Title 35. United States Code. §120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, §122, I acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations, §1.56(a) which occured between the filing date of the prior application and the national or PCT international filing date of this application.

(Application Serial No.) (Anmeldeseriennummer) (Filing Date) (Anmeldedatum) (Status) (patentiert, anhängig, aufgegeben) (Status) (patented, pending, abandoned)

(Application Serial No.) (Anmeldeseriennummer) (Filing Date) (Anmeldedatum) (Status) (patentiert, anhängig, aufgeben) (Status) (patented, pending, abandoned)

Ich erkläre hiermit, dass alle von mir in der vorliegenden Erklärung gemachten Angaben nach meinem besten Wissen und Gewissen der vollen Wahrheit entsprechen, und dass ich diese eidesstattliche Erklärung in Kenntnis dessen abgebe, dass wissentlich und vorsätzlich falsche Angaben gemäss Paragraph 1001, Absatz 18 der Zivilprozessordnung der Vereinigten Staaten von Amerika mit Geldstrafe belegt und/oder Gefängnis bestraft werden koennen, und dass derartig wissentlich und vorsätzlich falsche Angaben die Gültigkeit der vorliegenden Patentanmeldung oder eines darauf erteilten Patentes gefährden können.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true, and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

German Language Declaration

VERTRETUNGSVOLLMACHT: Als benannter Erfinder beauftrage ich hiermit den nachstehend benannten Patentanwalt (oder die nachstehend benannten Patentanwälte) und/oder Patent-Agenten mit der Verfolgung der vorliegenden Patentanmeldung sowie mit der Abwicklung aller damit verbundenen Geschäfte vor dem Patent- und Warenzeichenamt: *(Name und Registrationsnummer anführen)*

POWER OF ATTORNEY: As a named inventor, I hereby appoint the following attorney(s) and/or agent(s) to prosecute this application and transact all business in the Patent and Trademark Office connected therewith. *(list name and registration number)*

And I hereby appoint

Messrs.
James D. Halsey, Jr. (Reg. No. 22,729); Harry John Staas (Reg. No. 22,010); David M. Pitcher (Reg. No. 25,908); John C. Garvey (Reg. No. 28,607); J. Randall Beckers (Reg. No. 30,358); William F. Herbert (Reg. No. 31,024); Richard A. Gollhofer (Reg. No. 31,106); Mark J. Henry (Reg. No. 36,162); Paul I. Kravetz (Reg. No. 35,230); Gene M. Garner II (Reg. No. 34,172); Michael D. Stein (Reg. No. 37,240); Todd E. Marlette (Reg. No. 35,269); Norman L. Ourada (Reg. No. 41,235); Deborah S. Gladstein (Reg. No. 43,636); Jon H. Muskin (Reg. No. 43,824); Stephen Boughner (Reg. No. 45,317); John H. Stowe (Reg. No. 32,863); C. Joan Gilsdorf (Reg. No. 43,635); Mehdi Sheikerz (Reg. No. 41,307); James G. McEwen (Reg. No. 41,983); Michael J. Badagliacca (Reg. No. 39,099); Alicia M. Choi (Reg. No. P-46,621); Jon F. Hadidi (Reg. No. 46,427); and William M. Schertler (Reg. No. 35,348 (agent)).

Telefongespräche bitte richten an:
(Name und Telefonnummer)

Direct Telephone Calls to: *(name and telephone number)*

(202) 434-1500
Ext. ________________

Postanschrift:

Send Correspondence to:

Staas & Halsey LLP
700 Eleventh Street, N.W.
Washington, D.C. 20001
U.S.A.
Customer No. 21171

180

200

Voller Name des einzigen oder ursprünglichen Erfinders: FRIES, Steffen 26/02/2001	Full name of sole or first inventor:
Unterschrift des Erfinders Datum Steffen Fries	Inventor's signature Date
Wohnsitz D-81677 München, Germany DEX	Residence
Staatsangehörigkeit Bundesrepublik Deutschland	Citizenship
Postanschrift Wagenbauerstr. 5	Post Office Addess
D-81677 München Bundesrepublik Deutschland	
Voller Name des zweiten Miterfinders (falls zutreffend): EUCHNER, Martin	Full name of second joint inventor, if any:
Unterschrift des Erfinders Datum Martin Euchner 26-03-2001	Second Inventor's signature Date
Wohnsitz D-81737 München, Germany DEX	Residence
Staatsangehörigkeit Bundesrepublik Deutschland	Citizenship
Postanschrift Lorenzstr. 2	Post Office Address
D-81737 München Bundesrepublik Deutschland	

(Bitte entsprechende Informationen und Unterschriften im Falle von dritten und weiteren Miterfindern angeben).

(Supply similar information and signature for third and subsequent joint inventors).